UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

| | |
|---|---|
| **LORI MARCHAND** and **MONICA DEPINA**, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br>v.<br><br>Deloitte Consulting LLP,<br><br>Defendant. | Case No. _____<br><br>CLASS ACTION<br><br>JURY TRIAL DEMANDED |

# CLASS ACTION COMPLAINT

Plaintiffs Lori Marchand and Monica DePina ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant Deloitte Consulting LLP ("Deloitte" or "Defendant"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach of RI Bridges. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

## NATURE OF THE ACTION

1. This class action arises from the massive data breach of the RI Bridges computer software system ("RI Bridges"), used for providing the state's government assistance to Rhode Island residents, such those enrolled in SNAP, Medicare, Temporary Assistance for Needy Families, and healthcare purchased through the state's HealthSource RI.

2. The breach occurred in early December, when an international ring of hackers gained access to the state's online portal for obtaining social services, providing hackers access

to confidential data kept in the RI Bridges software system, including the private information ("Private Information") of anyone who may have received state assistance since 2016 ("Data Breach"). Information that is subject to the hack includes among other things, Class Members names, addresses, dates of birth, social security numbers and certain banking information.

3. Defendant Deloitte is the third party vendor, which maintains a contract with the State of Rhode Island and is primarily responsible for protecting the confidential and private data or Rhode Islanders using the portal, and was specifically responsible for running the systems and protecting Class members' confidential and private data. Deloitte's actions and the Data Breach are presently under investigation by the State of Rhode Island directed at determining why Deloitte failed to have stronger cybersecurity measures in place which enabled the Data Breach and ransomware attack.

4. As a consequence of the Data Breach and ransomware attack over 650,000 Rhode Islanders are at risk of having their identities stolen, or their personally identifiable information ("PII") and protected health information ("PHI").

5. The Data Breach has not only exposed the PHI and PII of Plaintiffs and Class Members to a third party which can now sell or exploit that information, but also disabled some Class Members from timely receiving their government assistance.

6. According to an announcement by the Rhode Island government, Deloitte launched an investigation into the Data Breach and confirmed that an unauthorized actor accessed the system on December 5, 2024, and that the hacker may have copied and exfiltrated certain files containing Plaintiffs' and Class members' PII and/or PHI.

7. In response, Deloitte immediately implemented additional security measures—measures which likely should have already been in place.

8. On December 10, 2024, the State of Rhode Island received confirmation from Deloitte based upon a screen shot of file folders sent by the hacker to Deloitte, that there had been a breach and on December 11, 2024, Deloitte confirmed that there is a high probability that the implicated folders contain personally identifiable information from RI Bridges.

9. On December 13, 2024, Deloitte confirmed that there was malicious code present in the system and the State directed Deloitte to shut down RI Bridges to remediate the threat.

10. Despite learning of the Data Breach on about December 5, 2024, and determining that PHI and PII was involved, Class Members only recently received notice in the form of texts of the data breach and from the RI Bridges system and the State of Rhode Island—not Defendant.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

12. Upon information and belief, Deloitte and its subcontractors were aware that the RI Bridges system was vulnerable to an unauthorized third party attack and data breach through audits by the Rhode Island State auditor, among other things, and through lawsuits, complaints and other issues which had plagued the RI Bridges system since its institution in Rhode Island. Nonetheless, Deloitte failed to take adequate measures and institute sufficient cybersecurity protections leaving the RI Bridges system vulnerable to a third-party intrusion and hack.

13. Through its contract with the State of Rhode Island, and the fact that it collected Private Information of State residents on government assistance, which it did for profit and for hundreds of millions of dollars paid by the State of Rhode Island, it had duties to users of the system to sufficiently protect their Private Information from unauthorized third-party access and

the ensuing damage. Nonetheless, Deloitte failed to take steps to institute adequate measures to prevent the Data Breach and left the RI Bridges system vulnerable to a third-party attack.

14. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

15. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained by Defendant on RI Bridge's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, particularly through audits performed by the State of Rhode Island, and Deloitte's history of malfunctions with the RI Bridges system. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

16. Defendant disregarded the privacy and property rights of Plaintiffs and Class Members, by inter alia, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate and complete notice of the Data Breach.

17. Plaintiffs' and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

18. With the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

19. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft, as well as sustaining damage by failing to timely receive their government assistance.

21. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

22. Accordingly, Plaintiffs bring this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Deloitte's unlawful conduct.

23. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

**PARTIES**

24. Plaintiff Lori Marchand is a resident of Rhode Island, residing in Cumberland, Rhode Island. Plaintiff and her children receive benefits through Medicaid, and she has had to submit her PII and PHI to Medicaid in order to obtain Medicaid benefits for her children.

25. Several weeks ago, Plaintiff received an email from the State of Rhode Island indicating to her that her PII or PHI had been subject to the Data Breach.

26. Since the Data Breach, Plaintiff has experienced an increase in spam calls, and calls from persons pretending to be from the Rhode Island Department of Human Services ("DHS"), who apparently have her telephone number, when she has not provided that information to the Department. She has also experienced an increase in unwanted emails.

27. Plaintiff Monica DePina is a resident of Rhode Island, residing in Cranston, Rhode Island. Plaintiff has received Medicaid benefits through the RI Bridges system and submitted her PII to the system to obtain those benefits.

28. Several weeks ago, Plaintiff received a notice from the State of Rhode Island Department of Administration with an RIBridges Alert, indicating that her personal information may have been impacted by the Data Breach, advising her to take steps to protect herself, and providing her with a link to follow with the steps to take to secure such protections.

29. Since the Data Breach, Plaintiff DePina has experienced suspicious telephone calls, in some cases with no caller identification, some of which threatened her and her family, indicating that she was under investigation.

30. As a consequence of the Data Breach and the suspicious telephone calls and other communications she has received, Plaintiff DePina has put a freeze on her credit, and has monitored her accounts.

31. Deloitte Consulting LLP is a Delaware limited liability company organized and headquartered in New York, New York. Deloitte's principal place of business is located at 30 Rockefeller Plaza, New York, New York 10112. Defendant can be served through its registered agent at: 222 Jefferson Boulevard, Ste. 200, Warick, Rhode Island 02888.

**JURISDICTION AND VENUE**

32. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

33. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a foreign registered limited liability company; it maintains an office in Rhode Island; and committed tortious acts in Rhode Island.

34. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Deloitte has the most significant contacts pursuant to the claims of this matter.

## BACKGROUND

### Deloitte was on Notice that the RI Bridges System was Vulnerable to Attack

35. For more than a decade, Rhode Island's technology infrastructure for much of its human services and health systems has depended upon Deloitte. For much of that time, the program, first called UHIP and now called RIBridges, has been marred by errors, lawsuits and investigations, with the system requiring more and more state funding while failing to adequately provide the necessary services or protection of the private information that it collected.

36. The initial roll out of the system in 2016, for instance, was disastrous, with the only a half-baked system being launched, leaving some of the State's most vulnerable citizens—children, the elderly, the disabled and the needy—without support. The roll out was, however, the largest IT project in Rhode Island's history eventually costing it over $300 million—over $200 million more than its initial estimate. By 2017, Rhode Island's then governor, Gina Raimondo, sought to withhold millions of dollars in payments to Deloitte due to the lack of functioning of the system.

37. Deloitte was already aware of the potential problems with the system, as it had already come under fire with the same system in Kentucky and thus was on notice of issues with the system.

38. Two years later, audits performed by the Office of the Auditor General of Rhode Island demonstrated serious failures by the system and by Deloitte, including, for instance, the payment of $11 million to over 10,800 dead people in 2019.

39. The Auditor issued a 443 page report that found a number of material failures that were tied to the State's computer system.

40. In 2023, the Auditor found that the system lacked certain internal control deficiencies, and that the State was relying on Deloitte and its subcontractor to oversee certain IT security functions over the system, and that the reports performed by them were insufficient. (Audit Report at p.364).

41. Despite knowing that the system was materially flawed, in the regular course of its business, Deloitte collected, and maintained the PII and PHI of recipients of state benefits through the RI Bridges system without instituting sufficient measures to keep that information private and to prevent that confidential and private information from being accessed by unauthorized third parties.

42. Deloitte knew, should have known, or was reckless in not knowing that the RI Bridges systems was vulnerable to an attack, but failed to fulfill its duty in taking steps to shore up the system, preventing such an attack.

**Deloitte's Privacy Policy**

43. Deloitte promises in it its Privacy Policy that it is "committed to protecting your privacy"[1].

44. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, Deloitte promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. Deloitte is aware of and had obligations created by HIPAA, FTCA, contract, industry standards, state law and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[1] https://www.deloitte.com/global/en/legal/privacy.html (last accessed n December 27, 2024).

45. Plaintiffs and the Class Members, as consumers, relied on the promises and duties of Deloitte to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

46. Consumers, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, especially when Social Security numbers and private health information are involved.

47. In the course of their dealings, Plaintiffs and Class Members provided Deloitte (through RI Bridges) with all or most of the following types of Private Information:

a. First and last names;

b. Home addresses;

c. Dates of birth;

d. Financial information;

e. HIPAA protected information relating to medical history and health insurance;

f. Photo identification and/or driver's licenses;

g. Email addresses;

h. Phone numbers; and

i. Social Security numbers.

48. Deloitte had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure to third parties which it failed to do despite being on notice of material issues regarding the RI Bridges system, particularly through audit by the Rhode Island State Auditor.

49. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Deloitte that included the Private Information of Plaintiffs and Class Members.

50. Deloitte admits that the files exfiltrated from Deloitte contained at least the following information of Plaintiffs and Class Members: names, addresses, dates of birth, banking information and Social Security numbers.

51. Upon information and belief, the Private Information stored on Deloitte's network was not encrypted.

52. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

53. As a result of the Data Breach, Rhode Island and Deloitte now encourages Class Members to take steps to mitigate identity theft, a tacit admission of the imminent risk of identity theft faced by Plaintiffs and Class Members.

54. Rhode Island and Deloitte is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

55. Deloitte had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

56. Deloitte could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII and

increasing the cybersecurity protections for the RI Bridges system and properly and completely monitoring the system as it was required to do.

**The Data Breach**

57. As a consequence of Deloitte's failures, its breach of contract, its breach of its Privacy Policy and its duties to Plaintiffs and Class members, unauthorized third parties now have access to Plaintiffs' and Class member's Private information.

58. On December 5, 2024, Deloitte became aware of a cyberattack to its servers. Deloitte notified the Rhode Island State government on December 13, 2024 of a major security threat. As a result, RIBridges systems were suspended and taken offline to address the cyberattack.[2]

59. News reports indicate that an unauthorized actor accessed Deloitte's network sometime around December 5, 2024, and was able to extract certain data from the network.

60. Deloitte claims that any "any individual who has received or applied for health coverage and/or health and human services programs or benefits could be impacted by this breach."

61. The programs and benefits that have been affected by this breach include:

- Medicaid,
- Supplemental Nutrition Assistance Program (SNAP),
- Temporary Assistance for Needy Families (TANF),
- Child Care Assistance Program (CCAP),
- Health coverage purchased through HealthSource RI

[2] https://admin.ri.gov/ribridges-alert (last accessed Dec. 27, 2024).

- Rhode Island Works (RIW),
- Long-Term Services and Supports (LTSS), and
- General Public Assistance (GPA) Program.

62. Deloitte reported that some of the information breached contained: "names, addresses, dates of birth and Social Security numbers, as well as certain banking information."[3]

63. Customers of RIBridges have been unable to access their accounts through their online systems. Rhode Island residents applying for benefits with the State can only submit a paper application while the systems are down.

64. Plaintiff Marchand is an individual who receives benefits for her children through Medicare by using the RI Bridges system, and has been affected by the Data Breach. Had Plaintiff Marchand known that her information would not have been handled with proper care, she would never have entrusted her private information to Deloitte.

65. Plaintiff DePina is an individual who received benefits through Medicaid through the RI Bridges system. Had Plaintiff known that her information would not have been handled with proper care, she would never have entrusted her private information to Deloitte.

66. Plaintiffs Marchand and DePina have experienced anxiety since learning about the breach, as they are aware of the dangers of identity theft and fraud. As a result, Plaintiffs has contacted an attorney, and are monitoring their accounts in order to mitigate the impact of the breach.

67. Plaintiffs suffered actual injury from having their Private Information exposed as a result of the Data Breach including, but not limited to (a) damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiffs entrusted to

[3] *Id.* (last accessed Dec. 27, 2024).

Deloitte as a condition for healthcare services for her children and/or for Medicaid benefits; (b) loss of their privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

68. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

**Deloitte Had a Duty to Secure Class Members Private Information**

69. At all relevant times, Deloitte had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs sand Class Members when Deloitte became aware that their PII was compromised.

70. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

71. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

72. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Deloitte that included the Private Information of Plaintiffs and Class Members.

73. Deloitte admits that the files exfiltrated from Deloitte contained at least the following information of Plaintiffs and Class Members: names, addresses, dates of birth, banking information and Social Security numbers.

74. Upon information and belief, the Private Information stored on Deloitte's network was not encrypted.

75. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

76. As a result of the Data Breach, Rhode Island and Deloitte now encourages Class Members to take steps to mitigate identity theft, a tacit admission of the imminent risk of identity theft faced by Plaintiffs and Class Members.

77. Deloitte is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

78. Deloitte had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

79. Deloitte could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

**Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' PII**

80. Deloitte acquires, collects, and stores a massive amount of PII of Rhode Island residents seeking government assistance, and in some cases, insurance and Medicaid benefits.

81. By obtaining, collecting, and using Plaintiffs' and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

82. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

83. Plaintiffs and the Class Members who used and applied and received benefits through the RI Bridge's system, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information in order for Plaintiffs and Class members to be able to receive government assistance and benefits.

**The Data Breach Was a Foreseeable Risk of which Defendant Was on Notice**

84. Deloitte was on notice that the RI Bridges system was vulnerable to attack.

85. Moreover, it is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Deloitte, are well aware of the risk of being targeted by cybercriminals.

86. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

87. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[4]

88. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

89. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are

[4] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Dec. 5, 2024).

being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

90. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such address, remains the same."[5] In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[6]

91. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[7]

92. In light of high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

[5] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 5, 2024).

[6] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reportedin-2021-new-report-says/ (last accessed Dec. 5, 2024).

[7] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Dec. 5, 2024).

records, May 2020), Defendant knew or should have known that its computer network would be targeted by cybercriminals.

93. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

94. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to and the loss of critical information and data." [8] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[9]

95. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Deloitte failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

**At All Relevant Times Defendant Had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information**

96. At all relevant times, Deloitte had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard

[8] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scamsand-crimes/ransomware (last accessed Dec. 27, 2024).
[9] *Id.*

methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Deloitte became aware that their PII was compromised.

97. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

98. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

99. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

100. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims including Plaintiffs and the Class may continue for years.

**The Value of Private Information and the Effects of Unauthorized Disclosure**

101. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

102. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[12] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

[10] 17 C.F.R. § 248.201 (2013).

[11] *Id*.

[12] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed July 20, 2022).

103. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[13]

104. The ramifications of Deloitte's failure to keep Plaintiffs and Class member's Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

105. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

106. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [14] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[15]

107. Deloitte is offering a limited time offer for identity theft monitoring and identity theft protection. Its limitation is inadequate when Class members are likely to face many years of identity theft. Moreover, this type of inadequate protection place the burden to monitor and report suspicious activity on the Plaintiffs and Class members rather than Defendant.

---

[13] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed July 20, 2022).

[14] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed July 20, 2022).

[15] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accesses July 20, 2022).

108. Theses services are wholly inadequate to provide Plaintiffs and Class members with sufficient compensation and protection for the multiple years of ongoing theft identity and other damage that they will face as a consequence of the Data Breach.

109. The injuries to Plaintiffs and Class members were directly and proximately caused by Deloitte's failure to maintain or implement adequate data security measures for Plaintiffs and Class members.

**Deloitte Failed to Comply with FTC Guidelines**

110. Deloitte was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

111. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

112. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[17] The guidelines note that businesses should protect the personal customer information that they keep; properly

[16] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed July 20, 2022).

[17] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 20, 2022).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

113. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

114. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

115. Deloitte failed to properly implement basic data security practices. Deloitte's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

116. Deloitte was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. Deloitte was also aware of the significant repercussions that would result from its failure to do so.

**Concrete Injuries are Caused by Defendant's Inadequate Security**

[18] FTC, *Start With Security*, *supra* note 16.

117. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

118. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. Plaintiffs and other individuals whose PII was entrusted with Defendant understood and expected that, as part of that relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

119. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

120. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;

- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

121. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

122. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

123. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

124. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.

125. As a result of the Data Breach, Plaintiffs and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

## CLASS ALLEGATIONS

126. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

127. The Class that Plaintiffs seek to represent is defined as follows:

> **All persons whose Private Information was accessed by an unauthorized third party due to the Data Breach.**

128. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and subcontractor used by Defendant in performing its duties respecting RI Bridges, any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

129. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

130. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant has identified over 650,000 Rhode Island residents whose Private Information may have been improperly accessed in the Data Breach.

131. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs and Class

Members' Private Information;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' PII/PHI;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiffs' and Class Members' damages;

i. Whether Defendant violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

j. Whether Plaintiffs and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

k. Whether Defendant violated common law and statutory claims alleged herein

132. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members , because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

133. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect

Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

134. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

135. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

136. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the

limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is similar to that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

137. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

138. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

139. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs and Class and Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Complaint.

140. Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class and as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiffs and Class and Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class and Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

## CAUSES OF ACTION

### Count I
### NEGLIGENCE

130. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

131. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of the regular course of its business operations. Plaintiffs and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private

Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

132. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

133. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

134. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

136. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

137. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

138. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

139. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

140. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who received its services, which is recognized by laws and regulations, as well as common law.

141. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

142. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

143. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations, but also because Defendant is bound by industry standards to protect confidential Private Information.

144. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

145. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Private Information that was in Defendant's possession.

146. Defendant was in a special relationship with Plaintiffs and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class Members' Private Information. The harm to Plaintiffs and Class members from its exposure was highly foreseeable to Defendant.

147. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

148. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

149. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when

dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

150. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

151. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

152. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

153. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

154. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

155. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

156. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

157. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

158. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

159. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

**Count II**

**BREACH OF IMPLIED CONTRACT**

160. Plaintiffs re-allege and incorporate by the paragraphs above as if fully set forth herein.

161. Plaintiffs and Class Members were required to provide their PII and PHI to Defendant as a condition of receiving other services through the RI Bridges system for government assistance.

162. Plaintiffs and Class Members provided their PII to Defendant or its third-party agents in exchange for Deloitte's services or employment. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

163. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII and/or PHI under certain circumstances, none of which relate to the Data Breach.

164. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

165. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private

Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

166. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

167. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

168. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

169. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

170. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

171. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

172. As a direct and proximate result of Defendant's breaches of the implied contracts,

Class Members sustained damages as alleged herein.

173. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

174. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

175. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

**Count III**
**UNJUST ENRICHMENT**

176. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

177. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

178. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

179. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal

Information, and charging the State of Rhode Island for such services. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

180. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

181. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

182. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

183. Plaintiffs and Class Members have no adequate remedy at law.

184. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information,

which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

185. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

186. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

**Count IV**
**Declaratory Judgment**

187. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

188. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

189. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures

adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information.

190. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

191. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Deloitte continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Deloitte continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

192. The Court also should issue corresponding prospective injunctive relief requiring Deloitte to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

193. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Deloitte. The risk of another such breach is real, immediate, and substantial. If another breach at Deloitte occurs, Plaintiffs and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

194. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Deloitte if an injunction is issued. Among other things, if another massive data breach occurs at RI Bridges, Plaintiffs and Class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Deloitte of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Deloitte has a pre-existing legal obligation to employ such measures.

195. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Deloitte, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the

Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 30, 2024

**Respectfully submitted,**

/s/ Peter N. Wasylyk

Peter N. Wasylyk (RI Bar # 3351)
**LAW OFFICES OF PETER N. WASYLYK**
1307 Chalkstone Avenue
Providence, RI 02908
Telephone: (401) 831-7730
Facsimile: (401) 861-6064
Email: pnwlaw@aol.com

**THEGRANTLAWFIRM, PLLC**
Lynda J. Grant*
521 Fifth Avenue, 17th Floor
New York, NY 10175
Telephone: 212-292-4441
Facsimile: 212-292-4442
Email: lgrant@grantfirm.com

**KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.**
Gary S. Graifman*
Melissa R. Emert*
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Facsimile: 201-307-1086
ggraifman@kgglaw.com
memert@kgglaw.com

***Attorneys for Plaintiffs and the Class***

**pro hac vice or applications for admission to be filed*